

Board of Governors of the Federal Reserve System

**REPORT ON THE BOARD'S
IMPLEMENTATION OF CRITICAL
INFRASTRUCTURE PROTECTION**



OFFICE OF INSPECTOR GENERAL



BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

OFFICE OF INSPECTOR GENERAL

September 29, 2000

Board of Governors of the Federal
Reserve System
Washington, DC 20551

Dear Members of the Board:

Earlier this year, the Office of Inspector General began a review of the implementation of the *Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63* (PDD 63) by the Board of Governors of the Federal Reserve System (Board). We are conducting this review as part of a multiphased, governmentwide effort organized by the President's Council on Integrity and Efficiency (PCIE) and the Executive Council on Integrity and Efficiency (ECIE).¹ We have completed the first phase of our review and, in an effort to give timely feedback, we are providing this interim report of the Board's progress with its PDD 63 implementation efforts, including issues which we believe the Board and division management need to address.

BACKGROUND

Issued in May 1998, PDD 63 calls for a national effort to secure the nation's critical infrastructures. Critical infrastructures are the physical and computer-based systems essential to the minimum operation of the economy and government, and include telecommunications, banking and finance, energy, transportation, and essential government services. Advances in information technology have caused the infrastructures to become increasingly automated and interdependent and have created new vulnerabilities to equipment failures, human error, weather, and computer attacks. To address these threats, PDD 63 requires that each government department and agency prepare a plan to protect its own critical infrastructure, including inventorying its mission-essential assets and analyzing and reducing vulnerabilities. The federal government is expected to serve as a model to the rest of the country, and voluntary participation of private industry is sought, through public/private partnerships, to meet common protection goals.

¹ The President's Council on Integrity and Efficiency (PCIE), established by executive order, dated March 26, 1981, is comprised of all Presidentially appointed inspectors general and certain government officials. The Executive Council on Integrity and Efficiency (ECIE), comprised primarily of the inspectors general appointed by designated federal entity heads, was created by executive order on May 11, 1992. Both the PCIE and the ECIE have the same mission: to address integrity and efficiency issues that transcend individual government agencies and increase the professionalism and effectiveness of inspector general personnel throughout the government. I currently serve as Vice Chair of the ECIE.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our Phase I review objective was to evaluate the Board's planning and assessment activities for protecting critical, cyber-based infrastructures. Subsequent review phases will focus on implementation activities for cyber-based assets and on planning, assessment, and implementation activities for physical infrastructures. To accomplish our review objective for Phase I, we met with Board officials and staff responsible for performing infrastructure protection activities, reviewed pertinent documentation, and assessed initial planning efforts and public/private partnership activities. We reviewed the Board's internal operations with regard to PDD 63 implementation as well as the Board's oversight and regulatory responsibilities related to this issue. We conducted our review in accordance with generally accepted government auditing standards.

FINDINGS AND RECOMMENDATIONS

Overall, the Board has taken numerous steps to improve information security that will help to meet many of the PDD 63 requirements. For example, penetration studies—where outside contractors attempt to “hack” the Board's website—are being conducted on a regular basis. The security of the Board's website was rated “best in class” by the consultants, and the minor vulnerabilities found during the studies have been promptly addressed. Board staff has also actively participated in interagency and public/private partnership activities related to PDD 63.

Significant work remains, however, to complete the planning and assessment activities associated with the Presidential directive. Work on the Board's Critical Infrastructure Protection Plan (CIPP) was delayed to allow a concentrated effort to prepare for Y2K. Completion of the CIPP and the initial vulnerability assessments is presently targeted for November 2000. Although the Board will be able to build on its Y2K efforts in completing these activities, we believe that meeting this target date is an ambitious goal. Staff must first identify the processes supporting the Board's core missions and rank the processes by criticality to identify those which are fundamental to mission accomplishment. Then, staff must identify the specific assets necessary to support the critical processes. These critical assets will include information (both paper and cyber-based), people, and physical structures. Interdependencies between critical processes and assets must be analyzed and the associated vulnerabilities assessed; cost-effective steps should be taken as soon as possible to mitigate identified vulnerabilities. Going forward, the CIPP must also be updated on a regular basis to meet PDD 63 requirements.

- 1. We recommend that the Board (1) formally appoint a Chief Infrastructure Assurance Officer (CIAO) with adequate authority to effectively manage the Board's PDD 63 implementation program and (2) ensure adequate resources across the Board are assigned to support this effort.**

Completing the CIPP and the associated activities will require the involvement of various divisions and offices across the Board. We believe the Board needs a CIAO to provide for a coordinated, consistent approach to PDD 63 implementation. Although the Board's

Chief Information Security Officer has assumed the CIAO responsibility, a formal appointment has not been made. We believe that formally appointing a CIAO, with clearly defined authorities, responsibilities, and accountabilities will help promote cooperation and coordination among divisions in conducting planning, assessment, and (eventually) implementation activities. Successful completion of these activities will also require the identification and assignment of adequate resources. During our review, we noted that two positions were approved to support PDD 63 activities in the Division of Information Technology (IT). To fully meet PDD 63 requirements, however, most Board divisions will likely expend resources in planning, assessment, and implementation activities. The required resources should be reflected in all affected divisions' plans and budgets.

In reviewing the Board's implementation of PDD 63, we also looked at the directive's requirements in light of the Board's responsibilities related to Reserve Bank oversight and financial institution supervision. Similar to the Board's internal information security efforts, we found that steps have been taken to implement protection efforts across the System and to issue information security guidance to regulated financial institutions. We believe, however, that implementing the following recommendations will help ensure that PDD 63 requirements are adequately fulfilled within the Federal Reserve System and the banking industry.

2. **We recommend that the Division of Reserve Bank Operations and Payment Systems (RBOPS) continue to closely monitor Reserve Bank operations and ensure that appropriate steps, as outlined in PDD 63 and related guidance, are taken to mitigate risks for critical system processes.**

Board staff informed us that the Reserve Banks have taken many steps to protect their critical physical and information assets. Although the Reserve Banks are not directly subject to the formal planning and reporting requirements of PDD 63, many of these actions meet the directive's intent. Reserve Bank staff has also actively coordinated with law enforcement and with public and private entities on PDD 63 initiatives. To date, Board oversight has not required the Reserve Banks to engage in the formal planning and assessment process as envisioned by PDD 63. Board staff considers this to be a burdensome paperwork exercise in light of the many actions already taken by the Reserve Banks to protect their critical infrastructure. RBOPS staff also indicated that the division's oversight program already assesses asset protection controls and activities for both physical and cyber-based assets and that the areas reviewed by the oversight function encompass key objectives of PDD 63. The Reserve Banks play a critical role in the nation's payment system and perform unique duties as fiscal agents and depositories of the United States. We plan to more fully assess RBOPS oversight activities as part of subsequent phases of our work related to this directive.

3. **We recommend that the Board review existing guidance for regulated financial institutions and determine whether any additional guidance is appropriate in light of PDD 63.**

Over the years, the banking regulatory agencies have developed examination procedures and guidance documents which address many of the elements of PDD 63. More recently, we found that the agencies have developed proposed interagency guidelines for safeguarding customer information. While this guidance is being developed to implement Sections 501 and 505(b) of the Gramm-Leach-Bliley Act, the guidance also addresses many PDD 63 concerns. We also found that the Office of the Controller of the Currency recently independently issued comprehensive PDD 63 guidance that will help bankers implement adequate protection for critical operations and assets. We believe the Board should review the existing body of guidance in light of the directive's requirements and provide financial institutions that it regulates with additional guidance as appropriate. Two areas where we believe additional guidance may be warranted are incident reporting and information sharing responsibilities; both areas are key components of PDD 63. To help promote consistency among the financial regulators, we also believe that the Board should work with the Federal Financial Institutions Examination Council to develop uniform guidance for PDD 63.

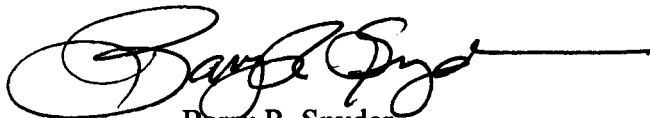
Going forward, we will continue to monitor the Board's planning and assessment activities and we will review implementation efforts for protecting critical assets. In addition to completing the PCIE/ECIE uniform review procedures, we plan to review the overall Board information security control environment for protecting cyber-based assets. The United States General Accounting Office (GAO) has been critical of government agencies for weak or nonexistent entitywide policies, procedures, and controls. Areas cited by GAO as deficient include security program planning and management; access, application development, and change controls; and business resumption planning and testing. To help ensure that Board information security controls are strong, we plan to review Board policies, procedures, and controls in these areas.

We have discussed the issues raised in this letter with the Staff Director for Management and officials in IT, RBOPS, and the Division of Banking Supervision and Regulation (BS&R). We also provided them a draft of the letter and have included their comments in appendix 1. Their responses indicate general agreement with the recommendations and identify actions that have been or will be taken regarding critical infrastructure protection. For example, the response from the Staff Director for Management indicates that he will initially serve as the Board's CIAO. We believe this will provide the Board's critical infrastructure program with the necessary authority to manage the Board's implementation efforts and ensure adequate resources are available. The response from the director of RBOPS identifies the division's active coordination efforts and ongoing oversight program, as well as the Reserve Banks' risk assessment and planning processes, as effective mechanisms for complying with the intent of PDD 63. The response from the director of BS&R highlights supervisory guidance that

incorporates, or will soon incorporate, PDD 63 information and notes the information sharing arrangements that are in the early stages of development within the financial industry. We plan to assess the actions identified in all three responses as part of our subsequent work related to this directive. Specifically, we will follow up on the recommendations presented in this report as part of our ongoing PDD 63 review activities.

This report is available on our web page and copies will be furnished upon request. We have provided status information to the PCIE/ECIE review team for inclusion in their summary report. We would be happy to answer any questions you may have or to discuss the information contained in this report in more detail. We appreciate the excellent cooperation staff have extended to us during this review.

Sincerely,

A handwritten signature in black ink, appearing to read "Barry R. Snyder", with a long horizontal line extending to the right.

Barry R. Snyder
Inspector General

cc: Mr. Stephen Malphrus
Ms. Louise Roseman
Mr. Richard Spillenkothen

Appendixes

Divisions' Comments

Appendix 1



BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

STEPHEN R. MALPHRUS
STAFF DIRECTOR FOR MANAGEMENT

DATE: September 28, 2000
TO: Barry Snyder
FROM: Steve Malphrus *SM*
SUBJECT: Draft Report on the Implementation of Critical Infrastructure Protection (A0002)

Thank you for the opportunity to respond to the August 24 OIG draft report (A0002) on critical infrastructure protection.

1. Recommendation One - We recommend that the Board (1) formally appoint a Chief Infrastructure Assurance Officer (CIAO) with adequate authority to effectively manage the Board's PDD 63 implementation program and (2) ensure adequate resources across the Board are assigned to support this effort.

Response - I will initially serve as the CIAO in order to organize the Board's program. I will also chair an interdivisional team consisting of participants from IT, RBOPS, BS&R and SS to share information and coordinate activities. I would invite the Inspector General's Office to participate on the task force in a liaison status. John Nash, IT, will serve as secretary of the task force.

2. Recommendation Two - See enclosed response from Louise Roseman
3. Recommendation Three - See enclosed response from Rich Spillokothan

Please call if you have questions or comments.

cc: Heidi Richards
Ken Buckley
Marianne Emerson
John Nash

(A0002)

Divisions' Comments (con't)

Appendix 1



BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

LOUISE L. ROSEMAN
DIRECTOR
DIVISION OF
RESERVE BANK OPERATIONS
AND PAYMENT SYSTEMS

September 28, 2000

Mr. Barry R. Snyder
Inspector General
Office of Inspector General
Board of Governors of the Federal
Reserve System

Dear Barry:

Thank you for the opportunity to respond to the August 24 OIG draft report (A0002) on the implementation of critical infrastructure protection. Recommendation number 2 of the report concerns steps being taken by this Division to ensure that the protection of the Federal Reserve System's critical infrastructure is appropriately addressed. It states:

2. **We recommend that the Division of Reserve Bank Operations and Payment Systems (RBOPS) continue to closely monitor Reserve Bank operations and ensure that appropriate steps, as outlined in PDD 63 and related guidance, are taken to mitigate risks for critical system processes.**

We are pleased that the OIG recognized that RBOPS has "actively coordinated with law enforcement and with public and private entities on PDD 63 initiatives." RBOPS has devoted substantial effort to promote national infrastructure protection efforts and has already undertaken significant steps to address PDD 63. Since 1988, we have represented the Federal Reserve on key government National Security and Emergency Preparedness (NS/EP) organizations focused on protecting telecommunication assets. Our administration of the NS/EP Telecommunications Service Priority and Government Emergency Telecommunications Service programs on behalf of Reserve Banks and private-sector payment system providers are examples of our commitment towards protecting critical infrastructures. We maintained a keen interest in the progress of the President's Commission of Critical Infrastructure Protection and its effect on the Federal Reserve cyber and physical protection programs. We were an early supporter of PDD 63 as we considered its objectives as perpetuating event management, business continuity, and threat assessment activities undertaken to prepare for Y2K. As a result, RBOPS staff worked closely with Department of Treasury officials to promote the Financial Services Information Sharing and Analysis Center by preparing a Board press release supporting this initiative last October and ensuring membership of the Federal Reserve. In November, as part of the FBI's Banking and Finance Key Asset training program, staff provided seminars on banking services and Federal Reserve operations to field agents. Early this year, RBOPS staff established a liaison role with

Divisions' Comments (con't)

Appendix 1

the FBI's National Infrastructure Protection Center (NIPC) and promoted participation of Reserve Bank offices in local Infragard chapters. Finally, RBOPS has worked with Reserve Banks to establish an efficient distribution process for communiqués from the FBI's Awareness of National Security Issues and Response (ANSIR) program.

We agree that PDD 63 requires that each government department and agency prepare a plan to protect its own critical infrastructure, including inventorying its mission-essential assets and analyzing and reducing vulnerabilities. We do not believe, however, that it dictates the methodology used by an agency to ensure that appropriate "formal" planning and assessment occurs. Because of the Federal Reserve's mission and its status as a public institution, Reserve Banks, over the years, have developed sound formal planning and assessment processes that are continually reviewed and revised to address new vulnerabilities. The Federal Reserve is recognized as a leader in cyber and physical security, including threat assessment, and business continuity. Two recent GAO reports, *Information Security and Risk Assessment Practices of Leading Organizations* (GAO/AIMD-00-33) and *Year 2000 Computing Crisis Federal Reserve has Established Effective Year 2000 Management Controls for Internal Systems Conversion* (GAO/AIMD-99-78), cited effective Federal Reserve risk assessment and disaster recovery practices. RBOPS assesses the extent to which Reserve Banks are effectively protecting the System's critical infrastructure as part of its oversight process. We believe that the Reserve Bank's infrastructure risk assessment and planning process and RBOPS' oversight effectively and efficiently complies with the intent of PDD 63.

We recognize the seriousness of critical infrastructure protection and do not consider efforts to ensure adequate protection to be burdensome for the Reserve Banks or this Division. We will continue to closely monitor Reserve Bank operations related to protection against physical and cyber-based threats. Our ongoing oversight review provides the necessary monitoring that was emphasized by the OIG in its recommendation. We do consider, however, any requirement that Reserve Banks engage in redundant or extraneous activities for the sake of process rather than substance to be burdensome and unnecessary.

I appreciate the opportunity to comment on your draft report. If you require additional information please contact Ken Buckley at (202) 452-3646 or Steve Sergek at (202) 530-6236.

Sincerely,

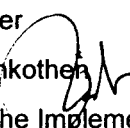


Divisions' Comments (con't)

Appendix 1

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

DIVISION OF BANKING SUPERVISION AND REGULATION

Date: September 14, 2000
To: Barry Snyder
From: Rich Spillenkother 
Subject: Report on the Implementation of Critical Infrastructure Protection

Thank you for the opportunity to review the OIG's draft *Report on the Implementation of Critical Infrastructure Protection*. We have also appreciated the opportunity to discuss this issue with your staff and better understand the elements of PDD 63 and the approach being taken by other agencies. BS&R has comments on the third recommendation only, which are provided below. In general, we concur with the recommendation.

3. **We recommend that the Board review existing guidance for regulated financial institutions and determine whether any additional guidance is appropriate in light of PDD 63.**

The Division of Banking Supervision and Regulation recognizes the need to review and update existing guidance in this evolving area to ensure that we provide supervised institutions with timely and useful information for protecting their operations, such as that contained in PDD 63. However, our understanding is that PDD 63 does not require the Board and other federal agencies to issue regulations or guidance to the industry. In fact, PDD 63 stresses the voluntary aspect of the program for the private sector.

Like PDD 63, the existing supervisory process focuses on protecting banks' critical operations and assets. We must remain sensitive to imposing additional, duplicative compliance burden on supervised institutions, particularly smaller institutions with very limited resources. As a result, we would expect to incorporate PDD 63 information into existing or anticipated supervisory guidance. For example, we anticipate issuing interagency guidance in the near future with the other FFIEC agencies in conjunction with the new information security standards (currently in proposed form) required under the Gramm-Leach-Bliley Act. We have met with and received input on the new standards from staff of the Critical Infrastructure Assurance Office, which, as you know, is officially responsible for implementing PDD 63. We are also in the process of updating existing interagency bank examination procedures for information security.

In addition, incident reporting for computer intrusions and other criminal activity is comprehensively covered in the agencies' newly revised suspicious activity report issued by the Board, as well as the other banking agencies, on June 19, 2000, and we would not anticipate issuing additional guidance in that area. Finally, it is our

Divisions' Comments (con't)**Appendix 1**

understanding that financial industry information sharing arrangements are in the early stages of development, and that the largest banking organizations are supporting these efforts. We believe it may be premature to direct smaller institutions to incur the costs of participating in these formal information sharing arrangements at this time.

Going forward, we would appreciate any suggestions you or your staff may have on other areas where we could incorporate PDD 63 guidance for institutions that we supervise.

cc: Steve Malphrus

Principal Contributors to this Report

Appendix 2

Gail Pinkepank, Senior Auditor and Auditor-in-Charge

Paul Sciannella, Auditor

William Mitchell, Program Manager